United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, and the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Friday,
October 29, 1999

YEAR 2000 COMPUTING CHALLENGE

Federal Business Continuity and Contingency Plans and Day One Strategies

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-40

Mr. Chairman, Ms. Chairwoman, and Members of the Subcommittees:

Thank you for inviting us to participate in today's hearing on the status of agencies' business continuity and contingency plans and Day One strategies. The public faces the risk that critical services provided by the government and the private sector could be disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors.

The risk to government operations due to these many potential points of failure can be mitigated by the development of effective business continuity and contingency plans. In addition, Day One strategies—developed either as part of business continuity and contingency plans or separately—can help agencies manage the risks of the rollover period during late December 1999 and early January 2000.

As requested, after a brief background discussion, today I will (1) discuss the state of the government's business continuity and contingency planning and (2) describe the status of Day One strategies.

Background

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.[1] We have also issued guidance to help organizations successfully address the issue.[2] Two of our publications—on business continuity and contingency

[1] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1997).

[2] *Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997); *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998); *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998); and *Year 2000 Computing Challenge: Day One Planning and Operations Guide* (GAO/AIMD-10.1.22, issued as a discussion draft in September 1999 and in final form in October 1999).

planing and on Day One planning and operations—provide guidance on the subject of this hearing.

Our business continuity and contingency guide describes the tasks needed to ensure the continuity of agency operations in the event of Year 2000-induced disruptions. The Day One guide provides a conceptual framework for developing a Day One strategy and reducing the risk of adverse Year 2000 impact on agency operations during late December 1999 and early January 2000.

Business continuity and contingency plans are essential. Without such plans, when failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Accordingly, in April 1998 we recommended that the President's Council on Year 2000 Conversion require agencies to develop contingency plans for all critical core business processes.[3]

Since 1998, the federal government has improved its approach to business continuity and contingency planning. The Office of Management and Budget (OMB) has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide for federal use. In addition, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13, OMB required agencies to submit high-level versions of these plans by June 15.

[3] *Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships* (GAO/AIMD-98-85, April 30, 1998).

As noted in our business continuity and contingency planning guide, a key element of such a plan is the development of a zero day or Day One risk reduction strategy. In testimony on January 20, 1999, we noted that the Social Security Administration had developed a Day One strategy and suggested that OMB consider requiring other agencies to develop such a plan.[4] In its September 1999 quarterly report, OMB subsequently required agencies to submit Day One strategies to OMB by October 15, 1999, as well as updated high-level business continuity and contingency plans.

While Work Remains, Agency Business Continuity and Contingency Planning Has Improved

Although more work remains, agency business continuity and contingency planning has evolved and improved since 1998. In March 1998, we testified that several agencies reported that they planned to develop contingency plans only if they fell behind schedule in completing their Year 2000 fixes.[5] In June 1998, we testified that only four agencies had reported that they had drafted contingency plans for their core business functions.[6] By contrast, in January 1999, we testified that many agencies had reported that they had completed or were drafting business continuity and contingency plans while others were in the early stages of such planning.[7] Finally, as we testified in August, according to an OMB official, all of the major departments and agencies had submitted high-level business continuity and contingency plans in response to OMB's May 13, 1999, memorandum.[8]

With respect to OMB's latest request for high-level plans, the 24 major departments and agencies and the U.S. Postal Service[9] have submitted updated business continuity and contingency plans. However, while the Department of the Treasury and the General Services Administration

[4]*Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions* (GAO/T-AIMD-99-50, January 20, 1999).

[5]*Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions* (GAO/T-AIMD-98-101, March 18, 1998).

[6]*Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress* (GAO/T-AIMD-98-205, June 10, 1998).

[7]GAO/T-AIMD-99-50, January 20, 1999.

[8]*Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Ensure Delivery of Critical Services* (GAO/T-AIMD-99-266, August 13, 1999).

[9]With respect to our analysis of high-level plans and the Day One Strategies, the term agencies will hereafter include the Postal Service.

reported that they had provided their plans to OMB, we did not receive these plans in time to include them in our analysis and, therefore, we analyzed 23 submissions.

While OMB's May 1999 memorandum directed agencies to describe their overall strategies and processes for ensuring the readiness of key programs and functions across the agency, it did not detail the format or reporting elements that the agencies were to follow. Accordingly, the plans vary considerably in terms of format and level of detail. Some agencies, such as the Departments of Justice and Labor described their general approach or strategy while others, such as the Departments of Education and Transportation, provided program or component agency specific plans that contained more detailed information. As an example of the first type of plan, the Social Security Administration's high-level plan identified broad areas of risk and general mitigation strategies and contingencies. However, as we testified in July,[10] the Social Security Administration has also completed local contingency plans to support its core business operations, and has obtained contingency plans for all state disability determination services as well as developed, in conjunction with the Department of the Treasury and the Federal Reserve, a Benefits Payment Delivery Y2K Contingency Plan. In contrast, the Department of Education provided OMB with its detailed contingency plans for its core business processes and their supporting systems.

In their high-level plans, some agencies provided details of the types of contingencies that could be implemented in the event of a Year 2000-induced failure. For example:

- The Social Security Administration described the risk that its field offices would be unable to issue certain types of payments due to Year 2000-related problems with automated support. In this event, the Social Security Administration stated that it would coordinate with the Department of the Treasury to address the problem. Further, in the event that it is known by December 1999 that enterprises such as local banks and/or the Postal Service were not ready to make delivery of payments in early January, the Social Security Administration stated that it would consider plans to issue payments early.

[10] *Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives* (GAO/T-AIMD-99-259, July 29, 1999).

- The Department of Education described the risk of a registration system failure at a school that prevents it from determining the title IV (student financial aid)[11] eligibility of its students. Education's risk mitigation/contingency activity if this occurs is threefold. First, Education stated that it will encourage schools to take steps to obtain registration and preregistration information before January 2000 for students beginning or continuing classes after January 1. Second, Education stated that it will encourage schools to develop other processes, including manual processes, for determining the enrollment status and eligibility of students who begin classes after January 1, 2000. Third, for students enrolled or preregistered in fall 1999 classes, Education will allow schools to package aid and credit students' accounts using fall 1999 enrollment or preregistration information, but not to disburse funds directly to students or parents. After the system is repaired, funds will have to be returned for any student who was ineligible. To implement these contingencies, Education stated that it would not enforce certain requirements and provided directions that a school is to follow (e.g., if a school makes a short-term loan to a student in lieu of paying a credit balance, the school may not charge the student interest on that loan).
- The Department of Veterans Affairs' Veterans Health Administration's contingency planning guidebook provides sample templates to be used as guides or models by its health care facilities. For example, to prepare for the potential problem that a facility would be unable to provide water in its inpatient wards for patients' needs and staff infection control, the facility could prepare locations for bottled water and stock waterless soaps. In the event that a failure actually occurred and action was needed, an assessment of the situation could be reported to a facility's command center, and bottled water centers established with control mechanisms.

All of the high-level plans in our review identified core business processes, as called for in our guide. For example, the Department of Labor identified and described seven core business functions: (1) benefits programs, (2) national employment and/or economic conditions tracking, (3) job training programs and employment assistance, (4) workers' benefits, (5) worker safety and health policy and oversight, (6) labor and employment policy and oversight, and (7) program support.

[11]Title IV of the Higher Education Act of 1965, as amended.

A key aspect of business continuity and contingency planning is validation, which evaluates whether individual contingency plans are capable of providing the needed level of support to the agency's core business processes and whether the plan can be implemented within a specified period of time. In instances in which a full-scale test may not be feasible, the agency may consider end-to-end testing of key plan components. Moreover, an independent review of the plan can validate the soundness of the proposed contingency strategy. We were able to identify 20 agencies that discussed their validation strategies in their high-level plan. These strategies encompassed a range of activities, including reviews, desktop exercises, simulations, and/or quality assurance audits.

In addition to reviewing high-level plans, we have assessed and reported on the business continuity and contingency planning of several agencies or their component entities and have found uneven progress. Some had instituted key processes while others had not completed key tasks. For example:

- As we reported on October 22, the Department of Justice's Federal Bureau of Investigation had made progress in its Year 2000 business continuity planning.[12] However, because Justice had not explicitly required and emphasized the importance of business continuity plans, the bureau had started late in undertaking its planning effort and was faced with a compressed time frame for testing and finalizing its plans. In addition, as of August 1999, the bureau did not have many of the management controls and processes needed to effectively guide its planning activities. For example, the bureau had not (1) developed a master schedule and milestones, (2) defined all of its core business processes, (3) assessed the costs and benefits of alternative continuity strategies, or (4) planned for the testing phase of its business continuity planning effort. We recommended improvements to the Federal Bureau of Investigation's planning activities, including that it establish and implement effective controls and structures for managing its business continuity planning. In commenting on our report, Justice indicated that it and the bureau had taken the first steps in implementing our recommendations.

[12] *Year 2000 Computing Challenge: FBI Needs to Complete Business Continuity Plans* (GAO/AIMD-00-11, October 22, 1999).

- In testimony last week we stated that, because of deficiencies in their contingency plans, the Department of State and the U.S. Agency for International Development lacked assurance that they could sustain their worldwide operations and facilities into the next century.[13] For example, State's business continuity and contingency plan did not identify and link its core business processes to its Year 2000 contingency plans and procedures, and the department had not yet tested its plans with Year 2000-specific scenarios. In the case of the U.S. Agency for International Development, we found that it had identified one core business process in its business continuity and contingency plan but did not identify or address other key agency functions. Moreover, the U.S. Agency for International Development provided little information on contingency planning activities for its missions, and it was unclear when the agency expected to complete its business continuity and contingency planning process.
- As we reported on October 14, the Department of Justice's Drug Enforcement Administration had managed its business continuity planning efforts in accordance with the structures and processes recommended by our guide, and had made progress toward completing its plans.[14] However, while progress had been made, the Drug Enforcement Administration still had many tasks to complete, with little time to address schedule slippages. For example, at the time of our review, it had not validated its business continuity strategy; defined, documented, or reviewed test plans; or prepared test schedules and test scenarios. The agency planned to complete testing of its plans by the end of November.
- The Internal Revenue Service's business continuity and contingency plans that addressed issuing refunds and receiving paper submissions were inconsistent in two key areas—performance goals and mitigating actions—as we reported in September.[15] This raised questions about whether these two plans provided sufficient assurance that the Internal Revenue Service had taken all necessary steps to reduce the impact of a potential Year 2000 failure. For example, neither of the plans specified

[13] *Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning* (GAO/T-AIMD-00-25, October 21, 1999).

[14] *Year 2000 Computing Challenge: DEA Has Developed Plans and Established Controls for Business Continuity Planning* (GAO/AIMD-00-8, October 14, 1999).

[15] *IRS' Year 2000 Efforts: Actions Are Under Way to Help Ensure That Contingency Plans Are Complete and Consistent* (GAO/GGD-99-176, September 14, 1999).

completion dates for the mitigating actions nor did the plans specify which individuals would be responsible for completing those actions. In response to our concerns, Internal Revenue Service officials agreed to make changes to these two plans and to review other business continuity and contingency plans for consistency and accuracy.

Business continuity and contingency plans are also key to ensuring that the government's highest priority programs are not adversely affected by the Year 2000 problem. In the case of some of the government's essential programs, not only is it important that the federal government have effective plans but their partners (such as states) must also have such plans in order to ensure program continuity. Accordingly, in its March 26, 1999, memorandum designating the government's 42 high-impact programs, such as food stamps (OMB later added a 43rd high-impact program), each program's lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work.

Our reviews have shown that some high-impact programs are farther along than others with respect to business continuity and contingency planning. For example:

- Yesterday we testified on the contingency planning progress of the Department of Veterans Affairs' two high-impact programs, benefits and health care.[16] The Veterans Benefits Administration's regional offices and Veterans Health Administration's medical facilities have completed their business continuity and contingency plans but testing is incomplete. Only 5 of 58 Veterans Benefits Administration regional offices had completed testing of their business continuity and contingency plans (all are now required to complete testing by November 15). In addition, while all of the Veterans Health Administration's medical facilities completed emergency power drills,

[16] *Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs* (GAO/T-AIMD-00-39, October, 28, 1999).

other portions of their plans, such as the possibility of water and gas shortages, have not been tested.

- On October 6, we testified on the readiness status of the 10 high-impact state-administered federal programs, including the business continuity and contingency plans being developed by the states for these programs.[17] With respect to the three such programs overseen by the Department of Agriculture's Food and Nutrition Service (e.g., food stamps), it was unclear whether all states had adequate plans to ensure the continuity of these programs. Indeed, as of September 15, Food and Nutrition Service officials told us that only two states had submitted suitable contingency plans.

In the case of the Department of Health and Human Services' Health Care Financing Administration's (HCFA) Medicaid program, of the 33 states and two territories that had been reviewed by a business continuity and contingency plan contractor, 11 were high risk, 11 were medium risk, and 13 were low risk. Regarding the five high-impact programs of the department's Administration for Children and Families administered by the states (e.g., Temporary Assistance for Needy Families), business continuity and contingency planning was one of the most common areas of concern cited in 19 state assessment reports available as of September 27, 1999.

With respect to the Department of Labor's Unemployment Insurance program, a contractor rated states' business continuity and contingency plans from low to high in terms of their compliance with Labor's requirements for coverage of core business functions of benefits and tax systems. Based on the contractor's completed reviews, the quality of state plans varied widely. For example, according to Labor's contractor, (1) 23 benefits and 14 tax plans had a low/very low degree of compliance with Labor's requirements and (2) 9 benefits and 5 tax plans had a high degree of compliance with Labor's requirements.

[17] *Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs* (GAO/T-AIMD-00-9, October 6, 1999).

- In September, we reported that the Department of Agriculture's Food Safety Inspection Service had not established milestones for completing complementary business continuity and contingency planning with its partners for its food safety inspection high-impact program. The food safety high-impact program's partners include 25 states with approval to operate their own inspection programs.[18]
- As we testified on September 27, the Health Care Financing Administration (HCFA) continued to make steady progress on its agencywide and 29 internal business continuity and contingency plans for its high-impact Medicare program, but the status of contractor plans was unknown and the results of HCFA's reviews of managed care organizations' plans were not promising.[19] With respect to its internal plans, HCFA had completed an agencywide business continuity and contingency plan, but essential validation activities remained. Regarding the Medicare contractors plans, HCFA's contractor and our review both found that not all Medicare contractors have specified detailed procedures that are required for executing and testing their business continuity and contingency plans. In the case of the managed care organizations, as of September 2, 1999, HCFA had received plans from 310 of the 383 managed care organizations. Its review of these 310 plans concluded that 69 percent needed major improvement, 18 percent needed minor improvement, and 13 percent were reasonable.

Mr. Chairman, on October 26, 1999, we briefed your Subcommittee staff on the results of our review of 11 high-impact programs, performed at your request. We found mixed progress on the business continuity and contingency planning for these programs. For example, the Defense Finance and Accounting Service reported completing the development and testing of its business continuity plan for military retiree and annuity pay while the Immigration and Naturalization Service had not completed or tested the business continuity plan for its immigration program. In other cases, such as the Postal Service's mail delivery program, the business continuity plans had been prepared but testing was not completed.

[18] *Year 2000 Computing Challenge: Readiness of USDA High-Impact Programs Improving, But More Action Is Needed* (GAO/AIMD-99-284, September 30, 1999).

[19] *Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues* (GAO/T-AIMD-99-299, September 27, 1999).

One key aspect of business continuity and contingency planning that has not been adequately addressed is the potential cost of implementing plans. Our business continuity and contingency planning guide calls on agencies to assess the costs and benefits of identified alternative contingency strategies. Accordingly, we testified in June that OMB's assessment of agencies' high-level plans should consider whether agencies provided estimated business continuity and contingency plan costs and, if not, OMB should require that this information be provided expeditiously so that it can give the Congress information on potential future funding needs.[20]

OMB has not required agencies to provide estimates of their business continuity and contingency plans. Nevertheless, in their August 1999 quarterly reports, we identified five agencies that specified estimated costs for some aspects of their business continuity and contingency plan development and/or implementation. For example, the Department of Health and Human Services estimated that it would cost about $99 million to implement its business continuity and contingency plans and Day One strategies regardless of how the year 2000 affects its operations, but its estimate does not include the cost of invoking the business continuity and contingency plan. The Department of Education's quarterly report stated that, as of August 13, 1999, its business continuity and contingency plan preparation costs were estimated at $3.2 million, and estimated that it would cost $7.5 million in the event that all of the plans had to be implemented (which it believed to be of very low probability).

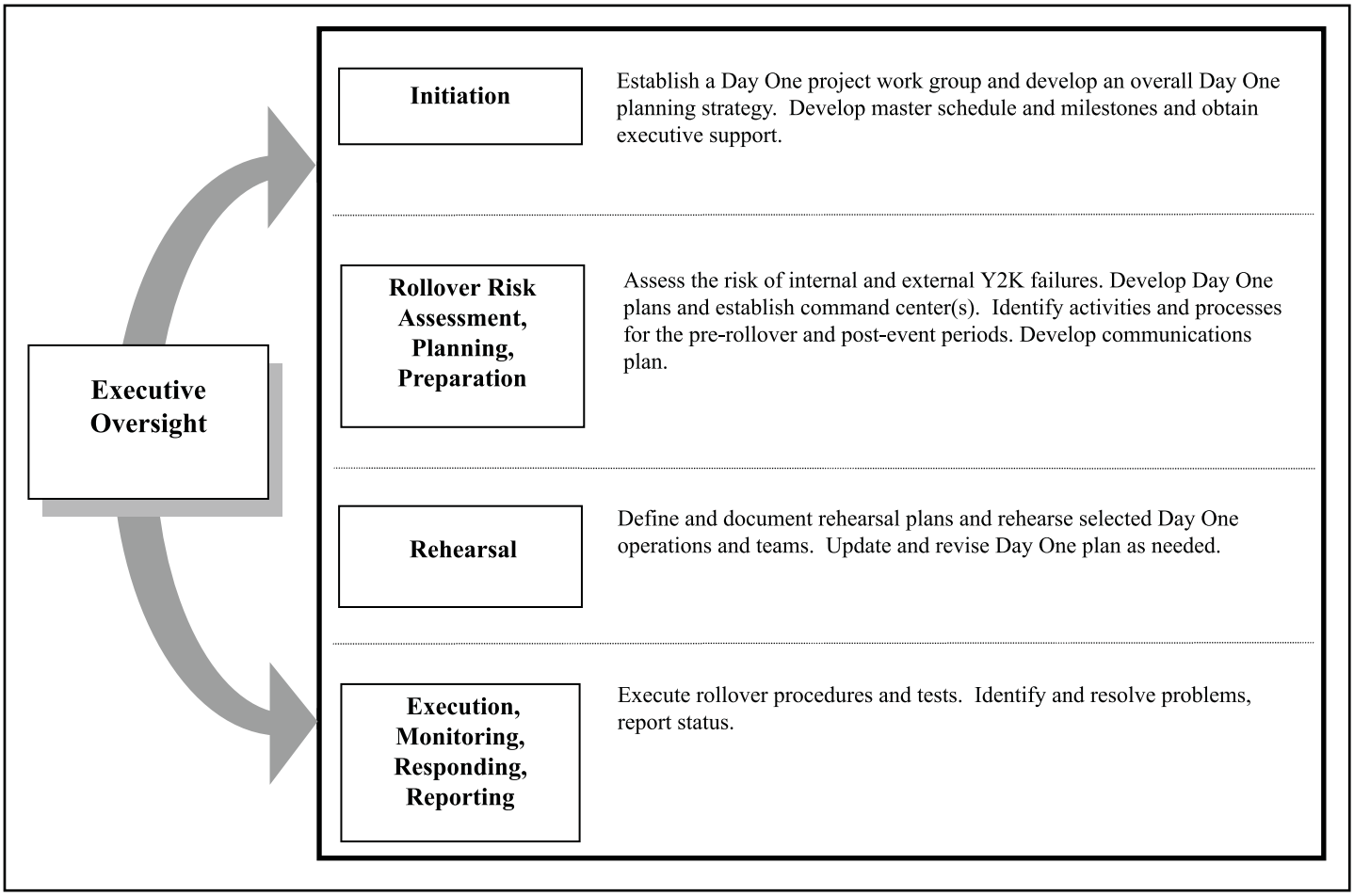
Day One Planning Is Ongoing

Day One strategies are necessary to reduce the risk to facilities, systems, programs, and services during the weekend of the critical rollover period. Accordingly, such strategies describe a wide range of complex, interrelated activities and geographically distributed processes that must be executed shortly before, during, and after the rollover. Earlier this month we issued a Day One strategy guide.[21] As shown in figure 1, the guide addresses four phases supported by executive oversight: (1) initiation, (2) rollover risk assessment, planning, and preparation, (3) rehearsal, and (4) execution, monitoring, responding, and reporting.

[20] *Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications* (GAO/T-AIMD-99-214, June 22, 1999).

[21] GAO/AIMD-10.1.22, October 1999.

Figure 1: Year 2000 Day One Planning and Operations Structure



In its September 1999 quarterly report, OMB required agencies to submit Day One strategies by October 15. OMB subsequently asked agencies to address seven elements in their plans: (1) a schedule of activities, (2) personnel on call or on duty, (3) contractor availability, (4) communications with the workforce, (5) facilities and services to support the workforce, (6) security, and (7) communications with the public. OMB also told the agencies to consider our Day One strategy guidance carefully. All agencies have submitted such draft or final strategies to OMB (either as part of their business continuity and contingency plan or as a separate document). However, while the U.S. Agency for International Development and the General Services

Administration reported that they had provided their plans to OMB, we did not receive these plans in time to include them in our analysis. Therefore, we analyzed 23 agencies' submissions.

Our review of the agency strategies found that about 40 percent (9 of 23) addressed all seven elements. For example, in our testimony yesterday we noted that the Department of Veterans Affairs addressed all of OMB's elements.[22] This department and its agencies had developed a Day One strategy that should help the department manage risks associated with the rollover period and better position itself to address any disruptions that may occur. For example, the strategy included a timeline of events between December 31 and January 1 and a personnel strategy and leave policy that identifies key managerial and technical personnel available to support day one operations.

With respect to specific elements, we were able to identify 15 agencies that included a schedule of activities and 17 that addressed staffing issues. Also, in a few cases, agencies addressed either OMB's internal communications element or external communication element but not both. Further, some elements were addressed in a general manner and/or indicated that more work needed to be completed. For example, one agency reported that it is developing procedures to ensure its ability to identify, report, and respond effectively to Year-2000 related events.

An important part of Day One planning is ensuring that the Day One strategy is executable. Accordingly, the Day One plans and their key processes and timetables should be reviewed and, if feasible, rehearsed. Our Day One strategy review found that 19 agencies discussed rehearsing their strategies, although some did not provide specific dates of planned or completed rehearsals.

In summary, business continuity and contingency plans and Day One strategies are key to managing and reducing the risks associated with the change to the year 2000. In the area of business continuity and contingency planning, noteworthy progress has been made since early 1998, although more work remains. With respect to Day One strategies, while about 40 percent of agencies addressed all of OMB's elements in their submissions, it is clear that much more work remains.

[22] GAO/T-AIMD-00-39, October 28, 1999.

Mr. Chairman, Ms. Chairwoman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittees may have at this time.

Contact and Acknowledgments

For information about this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at *willemssenj.aimd@gao.gov*. Individuals making key contributions to this testimony included Margaret Davis, Mirko Dolak, Jim Houtz, and Linda Lambert.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Mail
Postage & Fees Paid
GAO
Permit No. GI00